UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/107,618	06/30/1998	STEVEN M BLUMENAU	E0295/7066RF	8313

7590 01/23/2008

WOLF GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2211

EXAMINER
STRANGE, AARON N

ART UNIT	PAPER NUMBER
2153	

MAIL DATE	DELIVERY MODE
01/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/107,618
Filing Date: June 30, 1998
Appellant(s): BLUMENAU ET AL.

Richard F. Giunta
Reg. No. 36,149
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/29/07 appealing from the Office action mailed 10/18/06.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Ericson	US 6,061,753	May 9, 2000 (filed Jan. 27, 1998)
Boggs	US 5,959,994	Sep. 28, 1999 (filed Aug. 19, 1996)
Abadi	US 5,315,657	May 24, 1994
Yu	US 4,919,545	Apr. 24, 1990

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-4, 9-27, 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ericson (US 6,061,753) in view of Boggs et al. (US 5,959,994) further in view of Yu (US 4,919,545).

As per claim 1, Ericson teaches a data management method for managing access to a storage system between two devices coupled to the storage system through a network [col.1 "SCSI Fibre Channel bus or Ethernet based local area network"], the method comprising:

Receiving over the network at the storage system a request from one of the device [initiator – see col.3 lines 56-60];

Selectively servicing, at the storage system, the request responsive to configuration data indicating that the device [initiator] is authorized to access the portion of data [col.4 lines 4-25].

Ericson does not teach authenticating the request at the storage system to authenticate the device issuing the request. Yu teaches a security method for authorizing access by a process in source node to a resource in the network comprising encrypting an identifier of the requesting node using a key associated with the node, sending the encrypted key to the resource, decrypting the identifier at the resource node to verify the request [see abstract].

It is well known in the art at the time of the invention that SCSI peripherals may be distributed over wide area network using ATM and Fibre Channel. (See Boggs et al. US patent 5,959,994 col.2 lines 63-68, col.10 lines 8-22). Ericson specifically discloses that his invention is applicable to Fibre Channel protocols (col.6 lines 1-6). Hence, it would have been obvious for one of ordinary skill in the art to combine Boggs and Ericson because it would have enabled distributed access control to peripherals over wide area network.

Yu discloses that distributed network is venerable to identity spoofing (col.4 lines 56-65). Yu specifically discloses that security based on access control only is inadequate (col.1 lines 60-63, col.2 lines 7-10). Hence, Given the teaching of Yu, one of ordinary skill in the art would have been motivate to use both the access control security of Ericson together with authentication security of Yu to form an enhanced

security system to prevent both type of security breaches: unauthorized access and identification theft.

Therefore, it would have been obvious for one of ordinary skill in the art to combine the teaching of Yu with the storage system of Ericson as modified to authenticate that the represented device is the device making the request because it would have prevented access by a device masqueraded as an authorized device (see Yu col.3 line 29-35).

As per claim 2, Ericson teaches the storage system stores a plurality of volumes of data where configuration data stored in the storage system in a configuration table [look-up table] having identifier and information indicating which volumes are available to a device [col.4 lines 34-54].

As per claim 3, it is apparent Ericson as modified that the request would be forwarded to the storage system over the network.

As per claim 4, Ericson teaches using Fibre Channel [col.1 line 15, col.6 line 5]. It is apparent that a system with Fibre Channel would use Fibre Channel protocol.

As per claims 15-18, 21-22, 26-27 they are rejected under similar rationales as for claims 1-4 above. It is apparent that the process as modified would have computer program instruction stored on computer readable medium and the corresponding system for carrying out the method recited.

As per claims 11 and 30, Ericson teaches plural disk drives [RAID col.4 lines 5-15].

As per claims 12 and 29, Yu teaches validating that the request was not altered during transmit (col.3 lines 29-35).

As per claims 13 and 19-20, 24-25, Ericson teaches row with bitmap records corresponding to teach device authorized to access each of the corresponding ports [col.4 lines 40-53].

As per claims 14 and 23, Ericson teaches precluding service request responsive to configuration data [col.4 lines 47-50]. As per claims 9, 10, 31, 32, Ericson does not specifically disclose that the device is a host processor or file server. The type of device making the request would clearly have been a matter of design choice because it does not change the functionality of the storage system access control method taught by Ericson. Furthermore, Ericson teaches using the system may be used over a local area network [col.1 lines 15-16]. Official notice is taken that the usage of host processor and file server in a LAN or WAN is ubiquitous at the time of the invention. Hence, it would have been obvious host processor and file server requesting access to the storage system in Ericson as modified in order to provide file services to requesting clients.

Claims 33, 6-8, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ericson (US 6,061,753) in view of Boggs et al. (US 5,959,994) further in view of Yu (US 4,919,545) further in view of Abadi et al. (US 5,315,657).

As per claim 33, Yu teaches the request include a request access key (capability + signature 44), and verify with an expected key at the storage system (resource node) [see col. 6 line 50 to col. 7 line 44]. Yu does not teach sending an expected access key between the storage system and the requesting device. Yu teaches the resource node maintains a unique encryption key for each requesting node [col.7 lines 12-15, lines 50-56]. Yu does not specifically disclose how the resource node comes to possession of these unique keys. However, the method of providing encryption information to a destination node so that the destination node can encrypt data specifically targeted for the providing node is well known in the art. Abadi discloses using RSA cryptography to authenticate the identity of a requesting node by providing a public key to the destination and the destination returning to the requesting node data (i.e. the claimed expected access key) encrypted using that public key such that it can only be decrypted with the requesting node's private key. [See Abadi col.4 lines 50-68, col.5 lines 1 to col.6 line 8]. RSA cryptography is a well-known secured encryption standard and code fore implementing the encryption is readily available. Hence, it would have been obvious for one of ordinary skill in the art to modify Ericson and Yu to use RSA cryptography because it would have eased implementation of the encryption features

and to ensure difficulty for unauthorized device to gain access via theft of the access key.

As per claim 6, Yu teaches verifying the identified source by comparing the requested key to the expected key (col.3 lines 20-28).

As per claim 7, Yu clearly teaches encrypting using key associated with the device [col.7 lines 14-15].

As per claim 8, it is apparent that the system as modified would decrypt the access key using a decryption key provided initially by the device (the pubic key).

As per claim 34, Abadi teaches transferring of encryption information between the storage system and the device (the exchange of public key information [see Abadi col.4 lines 50-68, col.5 lines 1 to col.6 line 8]).

(10) Response to Argument

Regarding claims 1-4, 9-27 and 29-32, of which claims 1, 15 and 21 are independent, Appellants only present arguments to these claims collectively.

The various points raised by Appellants are summarized below, and each point is addressed individually by the Examiner.

Regarding claims 1-4, 9-27 and 29-32, Appellants present numerous arguments attacking the motivation to combine the cited references. Appellants essentially argue that there is no motivation to combine the authentication mechanism of Yu with the network system of Ericson since:

Ericson describes "a networked data storage system operating in a trusted environment" (Remarks, 10), specifically, a SCSI environment (Remarks, 17-20) and

"the nature of the SCSI environment and the details of the SCSI interface make it unnecessary and therefore undesirable to implement verification or authentication methods as disclosed by Yu" (Remarks, 17).

In reply, the Examiner respectfully disagrees with Appellants characterization of Ericson. Ericson discloses a method and system for controlling access to devices (targets 102) via a network bus 104 (fig. 1; col. 2, ll. 18-22; col. 3, ll. 50-52). At no point does Ericson specify whether the described system and method are in a "trusted environment". In fact, the disclosure does not even contain a single instance of the word s "trust" or trusted environment".

Ericson does disclose that one embodiment of the system is implemented using a SCSI bus (col. 3, ll. 53-56). Based on this disclosure, Appellants present pages of arguments directed to how the SCSI environment has no need for the authentication methods taught by Yu (Remarks, 18-20) since it is inherently trusted and secure due to its "local and contained" nature (Remarks, 18). However, even assuming that all of

these arguments are correct, Ericson discloses additional embodiments, and one of these embodiments was relied upon for the present rejection, as discussed below.

Ericson further discloses that the invention may be implemented using other known protocols, specifically mentioning Fibre Channel (col. 6, ll. 1-6). As admitted by Appellants (Remarks, 12) (agreeing that Fibre Channel "is sufficiently generic that it could be used in other system configurations that are untrusted"), Fibre Channel does not have the same inherent security found in a SCSI environment, since it is not "local and contained" and may be implemented over wide area networks (Boggs; col. 10, ll. 12-25). However, Boggs teaches that Fibre Channel is preferable to conventional parallel bus SCSI, since it allows peripherals to interface with an ATM switch (col. 2, ll. 67-67), allowing those peripherals to be connected via WANs, MAN, and LANs. Therefore, the use of Fibre Channel in Ericson is advantageous since it allows the peripherals to be connected over longer distances and interface with ATM switched, but disadvantageously eliminates the inherent security present in a SCSI environment, a disadvantage remedied by the teachings of Yu.

Yu teaches a method for preventing identity spoofing on a distributed network (col. 3, ll. 3-28). Yu teaches that distributed networks are vulnerable to identity spoofing (col. 4, ll. 56-65) and require security beyond conventional access control lists (col. 1, ll. 60-63; col. 2, ll. 7-10). Yu's method would have been an advantageous addition to the system taught by Ericson and Boggs since it would have eliminated identity spoofing on the Fibre Channel embodiment of Ericson.

In summary, Appellants rely on inherent properties of a particular embodiment (SCSI) of Ericson, an embodiment not relied upon in rejecting the appealed claims, as evidence attacking the motivation to combine Ericson with Boggs and Yu. The Examiner notes Appellants assertion that "[i]mplementation of the Fibre Channel protocol does not by itself convert a trusted environment into an untrusted environment" (Remarks, 15). While this is undoubtedly true, implementation of Ericson's system using Fibre Channel protocol does eliminate the inherent security found in a SCSI environment. As discussed above, Ericson does not describe a "trusted environment" and does not even use the term "trust" in the disclosure. Appellants' entire argument rests on the inherent security of a SCSI environment, which was not relied upon in rejecting the appealed claims. Since the prior art combination used to reject the appealed claims uses the Fibre Channel protocol, this inherent security is not present, and there is clear motivation to prevent identity spoofing on a distributed Fibre Channel network, as taught and remedied by Yu.

Ericson teaches a system for controlling access to devices via a network bus, and teaches that the invention may be implemented using Fibre Channel protocol. Boggs teaches that Fibre Channel protocol may be used to connect peripherals via distributed networks, such as WANs, and Yu identifies and remedies the problem of identity spoofing on distributed networks. The combined disclosure of these references teach all limitations present in Appellants' claims, which amount to nothing more than the combination of prior art elements, using known methods, to achieve a predictable result.

It is noted that Appellants have presented no separate arguments to any of the dependent claims encompassed by the first stated rejection, nor any arguments presented to the rejection of claims 6-8, 33 and 34, rejected under separate grounds. Accordingly, the Examiner has not addressed these issues beyond the discussion presented in the Grounds of Rejection section, above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Aaron Strange

1/16/08

Conferees:

Lynne H Browne
Appeal Practice Specialist, TQAS
Technology Center 2100

Glenton Burgess
Supervisory Patent Examiner
Art Unit 2153